Revisión: Primer parcial 2023 1C Criptografia - Matematica Aplicada

Encuestado

47 FRANCO JAVIER GARCETE

34:29
Tiempo para completar

26/30
Puntos

✓ **Correcto** 1/1 Puntos

1 / 1 pto

Más opciones para Respuestas

1

¿Cuál de los siguientes criptosistemas clásicos pertenece al tipo Transposición? *

- ○ Vernam
- ○ Vigenere
- ◉ Escitala ✓
- ○ César

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

2

¿Cuál de los cifradores clásicos cumple con el secreto perfecto de Shannon? *

- (●) Vernan ✓
- ( ) Playfair
- ( ) Hill
- ( ) Vigenere

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

3

¿Cuál sería una **desventaja** de los cifradores en bloque? *

- (●) Se debe leer todo el bloque ✓
- ( ) Hay una alta difusión en el criptograma
- ( ) Imposibilidad de introducir bloques sin detectarlos
- ( ) Baja difusión en el criptograma

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

4

¿En qué consiste un ataque analítico? *

- ○ Se prueban todas las claves posibles
- ◉ En la manipulación algebraica para reducir la complejidad ✓
- ○ En utilizar las debilidades estadísticas del diseño
- ○ No atacan el algoritmo, sino como fue implantado

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

5

La confusión consiste en: *

- ◉ La relación entre el texto cifrado y la clave sea lo más compleja posible ✓
- ○ Si se cambia un bit en el texto sin cifrar deberían cambiarse la mayor cantidad posible de bits en el texto cifrado
- ○ Si se cambia un bit en el texto sin cifrar debería cambiar la menor cantidad posible de bits del texto cifrado
- ○ Ninguna opcion es correcta

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

6

Seguridad en Wireless ¿Qué puede hacer un atacante Wireless? *

- ○ Monitoreo, captura y análisis pasivo de tráfico de red
- ○ Conseguir Accesos no autorizados
- ○ Robo de información
- ○ Actuar como Man in the Middle
- ◉ Todas las opciones son correctas ✓

✕ **Incorrecto** 0/1 Puntos

0 / 1 pto
Calificada de forma automática

7

Seguridad en Wireless- ¿Cuál no es un tipo común de EAP? *

- EAP-MD5
- EAP-Cisco Wireless (LEAP)
- EAP-TLS
- EAP-TTLS
- EAP-SSH ✓

✕ **Incorrecto** 0/1 Puntos

0 / 1 pto
Calificada de forma automática

8

Seguridad en Wireless - la siguente afirmacion "Con RADIUS toda la infraestructura Wireless está dentro del firewall corporativo" es: *

- Verdadero ✓
- Falso

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

9

Protocolos de seguridad en redes - ¿Cuál de las siguientes opciones **no** es una cualidad de IPSEC? *

- Permite soportar distintas aplicaciones.
- Puede cifrar y/o autenticar todo el tráfico a nivel IP
- Es transparente para aplicaciones y usuarios
- Permite armar VPN (Virtual Private Network)
- Es nativa en IP V4 ✓

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

10

Protocolos de seguridad en redes - ¿Cuál de las siguentes etapas **no** está al inicio de la comunicación en SSL – Secure Socket Layer? *

- Negociación de algoritmos a utilizar
- Intercambio de certificados y autenticación
- Negociación de clave simétrica de sesión
- Comprobacion de usuario active directory ✓

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

11

Protocolos de seguridad en redes - En SET – Secure Electronic Transaction las entidades deben instalar instalar el software. ¿Cuál opcion **no** es válida? *

- ○ Las entidades emisoras de las tarjetas de crédito
- ○ Los comercios adheridos
- ◉ Empresas externas de seguridad controladoras ✓
- ○ Los bancos que procesaban las operaciones

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

12

Protocolos de seguridad en redes - En Kerberos, ¿cuál de las siguientes opciones **no** es un objeto de seguridad? *

- Tickets
- Autenticadores
- MIME ✓
- Clave de sesion

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

13

Los números 624 y 180: *

- Son coprimos
- Tienen a 12 como máximo común divisor ✓
- Son primos
- Tienen a 4 como máximo común divisor

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

14

El inverso multiplicativo de 4 en Z_{23} es: *

- 8
- 6 ✓
- 20
- No tiene inverso multiplicativo

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

15

Postulados de Golomb - ¿Cuál de los siguientes **no** pertenece a los postulados? *

- Igual cantidad de unos que de ceros (+/- 1)
- Probabilidad de recibir un 1 o 0 es la misma
- Sin secuencias con mayor cantidad de información que otras
- Mayor cantidad de rachas que de huecos ✓

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

16

¿Cuál de las siguientes corresponde a una ventaja del cifrado en flujo? *

- (●) Alta velocidad de cifrado ✓
- ( ) Alta difusión en el criptograma
- ( ) Imposible introducir bits sin detectarlos
- ( ) Ninguna es correcta

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

17

¿Cuál de las siguientes variantes es más segura en la encripción Triple DES? *

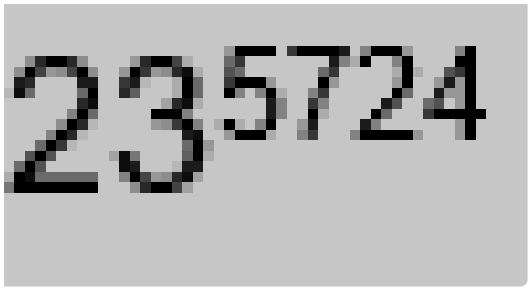
- (●) DES-EDE3 ✓
- ( ) DES-EDE2
- ( ) DES-EDE1
- ( ) DES-EEE4

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

18

El resto de dividir 23 elevado a 5724 por 3 es: *



- a2
- 1 ✓
- 0
- -1

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

19

¿Cuál de las siguientes características es provista por los sistemas simétricos? *

- No repudio
- Propagación
- Disponibilidad
- Confidencialidad ✓

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

20

El algoritmo de Diffie-Hellman es usado para: *

- Encripción de archivos
- No repudio
- Intercambio de llaves ✓
- Firma Digital

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

21

El cálculo de inverso multiplicativo *

- ( ) Es utilizado para aplicar el cifrado de información
- (•) Es utilizado para aplicar el descifrado de información ✓
- ( ) Es utilizado para realizar el intercambio de claves
- ( ) Ninguna es correcta

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

22

¿Qué concepto matemático usa como base para la encripción el algoritmo RSA? *

- ( ) Matemática discreta
- ( ) Problema del logaritmo discreto
- ( ) Curvas elípticas
- (•) Grandes números primos ✓

✕ **Incorrecto** 0/1 Puntos

0 / 1 pto
Calificada de forma automática

23

¿Cómo se llama al valor de longitud fija usado como huella digital en un mensaje? *

- (●) MAC
- ( ) Mensaje cifrado
- ( ) Hash ✓
- ( ) Firma Digital

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

24

¿Cuál de los siguientes puntos es verdadero sobre certificados digitales? *

- ( ) No pueden contener datos geográficos.
- ( ) Solo se pueden usar los tienen cargados la clave pública de la CA en los navegadores.
- ( ) Es un algoritmo criptográfico que permite generar una clave pública y una privada.
- (●) Prueba que el suscriptor de un certificado es quien dice ser. ✓

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

25

Sellado de tiempo – Time Stamping: Se aplica, entre otras cosas, para: *

- Establecer comunicación que dura un tiempo determinado
- Intercambio de clave
- Protección de la propiedad intelectual ✓
- Ninguna es correcta

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

26

¿Qué tipo de cifrador es el cifrador de Cesar? *

- Sustitución ✓
- Esteganografía
- Polialfabético
- Trasposición

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

27

¿Cuáles de los siguientes **no** se puede asegurar con criptografía? *

- Garantía de que un usuario es quien dice ser
- Almacenamiento seguro
- Comunicaciones seguras
- Garantía de que un mensaje llegue ✓

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

28

¿Cuál es el objetivo del proyecto eSTREAM? *

- Demostrar las debilidades de DES
- Demostrar las debilidades de LFSR
- Definir un algoritmo standard para el cifrado en flujo ✓
- Definir un algoritmo standard para el cifrado en bloque

✓ **Correcto** 1/1 Puntos

1 / 1 pto
Calificada de forma automática

29

El algoritmo elegido en el año 2000 como nuevo estándar de cifrado avanzado (AES): *

- Es de tipo Feistel
- Tiene un tamaño de clave fijo de 128 bits
- Usa Cajas S similares al DES ✓
- Originalmente se llamaba LUCIFER

✗ **Incorrecto** 0/1 Puntos

0 / 1 pto
Calificada de forma automática

30

El algoritmo ElGamal *

- Es un algoritmo simétrico
- Basa su seguridad en la dificultad de resolución del Problema del Logaritmo Discreto (PLD) ✓
- Basa su seguridad en la dificultad de resolución del Problema de la Factorización de Números Grandes (PFNG)
- Elimina la necesidad de tener un centro para distribuir llaves